Trust and security in the information society

SPECIFICS OF BLOCKCHAIN USE IN THE RUSSIAN FINANCIAL SECTOR WITHIN THE CONTEXT OF CYBERSECURITY AND CYBER IMMUNITY

Статья рекомендована к публикации членом редакционного совета А. А. Стрельцовым 25.12.2024.

Yudina, Tamara Nikolaevna

Doctor of economics, professor
Lomonosov Moscow State University, Faculty of global processes
Moscow, Russian Federation
orchidflower@list.ru

Kupchishina, Elena Valeryevna

PhD applicant
Lomonosov Moscow State University, School of public administration
Moscow, Russian Federation
sigrdriva@inbox.ru

Abstract

Blockchain in Russia is the key end-to-end digital technology, based on which the digital ruble is launched as fiduciary digital national money. Purpose: to explore the role of blockchain, quantum technologies and computers in building up cyber immunity in Russia. Results: the peculiarity of using blockchain in Russian financial sector is the creation of the fiat digital ruble, rather than cryptocurrencies. Conclusions: the original hypothesis of ensuring blockchain ecosystems and platforms cybersecurity, in response to increasing cybercrime, in view of Russian financial sector cyber immunity development, is proposed; Russia, like other countries, hasn't developed cyber immunity – "Quantum inoculation" is required.

Keywords

blockchain; Russian financial sector; cyber immunity

Introduction

The modern era of digital transformation based on cybernetization and internetization, the creation of a "digital civilization" is characterized by turbulence. The transition to a new technological order, based, among other things, on digital technologies, is accompanied by many threats and risks. Cyber fraud has become a pressing issue all over the world, so-called "digital bubbles" are inflating, there is a fierce struggle for technological leadership between IT-companies and states, and there is room for the growth of the shadow economy, whose representatives actively use cryptocurrencies. The answer to these challenges is to ensure the country's cybersecurity and, moreover, cyber immunity in the context of blockchain.

The article focuses on the specific problems of using blockchain in the financial sector of the Russian Federation economy from the point of view of cybersecurity and cyberimmunity. In Russia, relevant literature on blockchain and distributed ledger, which is the main end-to-end technology of the Russian digital economy, as well as the one of the other countries, is being introduced into the scientific fold in connection with quantum resistance "to attacks using the so-called relevant or significant quantum computer (Cryptographically Relevant Quantum Computer, CRQC)" (Petrenko, 2023). The solution to the problem of creating cyber immunity is becoming a subject of increasing importance.

https://doi.org/10.52605/16059921_2025_05_58

1 Theoretical and methodological foundations of blockchain

Blockchain has become the subject of a vast body of studies in the field of neo-institutional economic theory in the 2020s. Within the framework of the so-called Coasian paradigm P. de Filippi and S. Hassan identify the blockchain as a regulatory technology (De Filippi & Hassan, 2016), S. Davidson, J. Potts and others - as an institutional technology, through which decentralized transactions are implemented. According to their interpretation, this institutional technology allows reducing transaction costs and increasing the efficiency of economic systems and processes (Davidson, De Filippi, & Potts, 2018, p. 639-658). Russian researcher D.P. Frolov, developing this theoretical foundation from the position of post-institutionalism, and, precisely, from institutional assemblage theory point of view. The abovementioned theory defines blockchain as an institutional technology that not only reduces transaction costs, but also stimulates intermediaries to improve the quality of transactions, and also increases the supply and range of transaction services (Frolov, 2021, 21-36).

According to the report of the Central Bank of the Russian Federation "Development of the digital asset market in Russia", blockchain is positioned as "... one of the options for implementing a network of distributed ledgers, in which data is structured in the form of a chain (sequence) of cryptographically linked transaction blocks." This report notes that "each block contains an encrypted link to the previous one to ensure the immutability of records. According to the level of access, public, closed and hybrid networks of distributed registries are distinguished. The peculiarity of public networks is that anyone can become a member, and the data in such a network is open to any user. This ensures openness and transparency of operations. However, to ensure the anonymity of transactions, users are not identified by default. At the same time, public networks are characterized by risks associated with the quality of the program code and errors in it, the inability to restore access to the wallet if the password is lost, as well as difficulties associated with protecting the rights of users in court (for example, in terms of the execution of judicial acts, determination applicable law). Closed networks are characterized by the presence of a separate mechanism or procedure (regulation) for connecting new participants, and there may also be restrictions on the number and type of connected participants" (Bank of Russia, 2022b, p. 4).

Thus, from a theoretical and methodological viewpoint, there are various interpretations of blockchain in Russia and other countries of the world at the present time, used both directly in theory (for example, in neo-institutionalism) and in practice (for example, by the Central Bank of the Russian Federation, the Federal Tax Service of Russia).

2 Blockchain, cryptocurrency and central bank digital currencies (CBDC), smart contracts and "digital bubbles"

Blockchain is a distributed database consisting of a "chain of blocks". Block storage devices are not connected to a common server; they are stored and processed on many different computers. This is a kind of "digital workbook" in which the entries are unchanged thanks to the hashing mechanism – a unique set of alphabetic and numeric characters, where a change in one character entails a change in other blocks.

The main operating principle of this technology is the transparency of transactions performed, with the inability to change them for people who do not have authorized access to them. The idea is to create a self-replicating cryptocurrency that does not require the maintenance of third parties, i.e. financial institutions or banks - Bitcoin - prompted the development of digital blockchain technology. Humanity still uses the services of financial intermediaries who use the capabilities of "digital civilization" in their own interests.

The main feature of the blockchain is the transparency of the transactions, which is both the main principle of the implementation of this digital blockchain technology, and a large number of copies of all these transactions, which allows each participant in the transactions to view all the information on each step of the partners. This technology eliminates the possibility of adding a fake block or removing it from the chain. In fact, it is impossible to add something to the chain that should not be there. Thus, fraud, interference and attempts at illegal access, non-institutionalized entry and use of resources, and piracy are practically excluded. To attempt to gain unauthorized access to resources (hacking), it is necessary to hack the necessary previous block, the entire sequence of commercial transactions on this distributed ledger, not on one computer, but on millions at the same time, which is virtually impossible to do.

Miners mine cryptocurrency using the blockchain. The essence of mining is that computers located in various places around the globe carry out calculations and thus generate new blocks of the blockchain.

Indeed, the job of miners is to select from millions of combinations one single cache as the result of some mathematical transformation of a block from the previous block. The first of them will be rewarded with a certain number of virtual coins, for example, bitcoins, which participants in the transaction "pawn" as a commission when performing the transaction. The first to find the key is the one who is technically and technologically better equipped (has powerful equipment: a farm, video cards, etc.) for mining. Digital blockchain technology in the context of mining turns miners into many "central banks" who want to eliminate the only Central Bank of the country.

The almost sixteen-year history of the first cryptocurrency reproduction - Bitcoin, as well as other cryptocurrencies, has convincingly shown that blockchain technology has significant shortcomings. According to Russian analysts, "blockchain platforms do not solve performance issues; they, as a rule, do not allow processing a large number of transactions simultaneously. So, for example, in the Bitcoin network, the speed of confirming transactions in the blockchain does not exceed seven transactions per second, while, for example, the international payment system Visa can process up to 24 thousand transactions per second." Another, in our opinion, significant drawback is that "issues with combating money laundering and terrorism financing have not been resolved due to the presence of mechanisms that allow anonymizing transactions made in blockchain platforms (mixers, zero-knowledge proof protocols and other means of ensuring confidentiality)".

For the time being, an alternative to using blockchain digital technology has become the reproduction of digital fiat and/or fiat money. Thus, "many central banks are developing central bank digital currencies (CBDCs), which allow the technological advantages of private crypto assets to be realized while at the same time providing the guarantees inherent in fiat currency. The creation of CBDC by the Central Bank will help mitigate the risks caused by the lack of security and control by the state over cryptocurrencies, while simultaneously maintaining a number of advantages associated with the use of distributed ledger technology" (Bank of Russia, 2022a, p. 8).

However, blockchain cannot eliminate the intermediary, i.e. the Central bank when it comes to monetary transactions at the macro level. Bypassing Central Banks in transactions is dangerous for national finances. Capital can move across borders without the awareness of national banks.

Thus, if the rules are set not by the National Bank, but by digital blockchain technology, then this poses an even greater national financial danger.

That is why both Russian and Chinese national banks are now pushing for digital yuan and digital ruble. This is the centralization of digital fiat money, as opposed to the decentralization of cryptocurrencies as private quasi-money.

In accordance with K. Schwab's book "Shaping the Fourth Industrial Revolution", blockchain is characterized as a technology that, by ensuring the immutability and verifiability of information when transmitted from one exchange relationship party to another, makes transactions safe and transparent, all participants in the exchange relationships obtain full spectrum of rights, that, however, seems to be a rather controversial statement - at least in view of the uneven distribution of resources and the allocation of power (according to J. Robinson) (Robison, 1979, p. xi) among various participants in economic activity. It is obvious that the possibilities to influence on the market, as well as resources and production capacity, of a certain large transnational corporate structure that makes payments via blockchain, are much greater than, following K. Schwab, "individuals and small investors" (Schwab, 2018, p 110), individuals, small and medium-sized businesses. A striking example in this sense is JP Morgan, which for the purposes of client payments (clients include 80% of Fortune 500 firms) in 2019 initiated the functioning of its own cryptocurrency JPMCoin (Tjotkin, 2019).

Indeed, blockchain technology generally guarantees the transaction itself, not national cyber security. But without national security, the principles of freedom and justice in the Russian and global financial sectors cannot be ensured.

3 Cybersecurity and digital immunity: global and Russian experience

The statement on the transparency and full traceability of transactions carried out via blockchain does not stand up to the test of the practice of blockchain use in the financial sector. Otherwise, there would not have been a massive layer of crimes associated with the theft of cryptocurrencies, laundering of proceeds from illegal activities through them, and, accordingly, challenges for global and Russian regulators. The Bank of Russia, delving into the fabric of blockchain and cryptocurrencies in its documents, participating in the formation of a mechanism for ensuring cybersecurity (Yudina, Lemeshchenko, & Kupchishina, 2022,

p. 31-45), focuses the issues of identifying illegal activities (including terrorism financing) using mechanisms anonymization of transactions carried out through cryptocurrency mixers on blockchain platforms (Bank of Russia, 2022a, p. 8).

One of the responses to the challenges associated with opportunistic behavior in the context of blockchain, cryptocurrencies and fiat digital money is the development of international standards for combating money laundering, the schemes of which involve these virtual assets.

Analysis of global and Russian experience in the use of cryptocurrencies in the financial system demonstrated the need for a deep understanding of the risks associated with innovative technologies in the financial sector of Russia and the world, new mechanisms for transferring value through a "network of networks" (Internet), and the formation of international standards to combat money laundering and terrorism financing. In 2018, the Financial Action Task Force (FATF), an international intergovernmental organization, developed recommendations on the registration and licensing of cryptocurrencies, and highlighted the need to develop an approach based on assessing the level of risk, mechanisms for countering illegal activities carried out through virtual assets. By 2021, these recommendations, addressed by the intergovernmental organization to a wide range of participants in the financial sector, primarily national regulators, were supplemented with responsibilities for assessing the level of cryptocurrencies transactions risk for businesses whose activities involve such transactions (banks, brokers, etc.), compliance with the due diligence principle, especially when checking counterparties within a decentralized transaction. As part of the implementation of these measures, the Financial Action Task Force recommends that financial market participants use such sources of information as registers of government authorities containing information on the counterparties' beneficial owners, corporate registers, as well as databases of enforcement actions taken by supervisory authorities in relation to financial sector entities, court decisions, etc. as well as decisions of international bodies coordinating supervisory activities in the field of AML/CFT (IMF, World Bank, FATF, etc.) (FATF, 2021, p. 78-87).

For 2022 – 2024 period in the Russian Federation, with the participation of the banking community, 12 priorities for financial technologies development have been outlined, including "Development of blockchain technologies", a project aimed at creating the infrastructure of this technology, considered as the basis for innovation for the financial and non-financial markets, as well as "Safe financial market", a project aimed at developing mechanisms for ensuring cybersecurity and combating fraud (Bank of Russia, 2021, p. 13). As part of minimizing the risks of using blockchain in cybercrimes, as well as in laundering proceeds from crime, financing terrorism and the proliferation of weapons of mass destruction, the Russian financial sector, under the guidance of the Central Bank of the Russian Federation and Rosfinmonitoring, is developing a fairly strict approach to regulating cryptocurrencies.

In 2020, at the initiative of Rosfinmonitoring, the "Transparent Blockchain" project was included in the federal program "Artificial Intelligence", which implies the creation of a digital service for information exchange, analysis of new schemes for the illicit circulation of cryptocurrencies, and management of related risks. The developer of this service was the Lebedev Physics Institute (Kulikova & Koroljov, 2023, p. 8). The practical application of this tool demonstrates its effectiveness: in 2022, the supervisory authority received about 70 thousand reports of suspicious transactions. As a result, several dozen criminal cases related, incl. with corruption, brought to court (Vakhitova, 2023).

As a result of the blockchain use practice analysis in the Russia, a significant groundwork for conceptualizing a model for ensuring cybersecurity in the digital economy of Russian Federation has been identified. The impact of blockchain on the mechanism for ensuring cybersecurity in the Russian digital economy has not been fully determined. At the same time, regulators of the Russian financial sector are faced with an ambitious task - developing a substantive approach to identifying typologies (in fact, patterns of opportunistic behavior) of dubious transactions with cryptocurrencies.

The above can be considered as components of the digital immunity. Cyber immunity is defined by authors as a system of interrelated institutions: digital technologies as institutions, i.e. technological knowledge, skills, and abilities as the basis for technological rules (algorithms of actions), formal rules, and patterns of thinking and acting. The latter are able to reduce transaction costs connected with the actors' opportunistic behavior and ensure stable, constructive and effective functioning of the digital economy.

Conclusion

The main message. The specifics of using blockchain in the financial sector of the Russian economy from cybersecurity and cyberimmunity point of view is that, starting from August 1, 2023, the digital ruble has

been introduced into monetary circulation along with cash and non-cash money. Blockchain digital technology dictates the rules, that is why it becomes an institution.

The results, representing the novelty of the study, are as follows. First, the blockchain use specifics in the Russian financial sector is in the creation of fudiciary (or fiat) digital money - the digital rouble, rather than cryptocurrencies as private quasi-money. Secondly, cryptocurrency mining in Russia is institutionalized starting from the 1st of November, 2024. The Russian digital coins and tokens market is regulated by the Federal Law dd 31.07.2020 No. 259-FZ "On Digital Financial Assets". In Russia, an individual intending to engage permanently in cryptocurrency mining, is obliged to register as entrepreneur or to incorporate a legal entity. Currently, any individual engaged into cryptocurrency mining, provided the one pays for the electricity used, until then is considered to have the clean record. Third, providing the insight into the gap in existing theoretical and practical concepts of digital (cyber) immunity as an institutional "inoculation" for cybersecurity is important both for the theory and managerial practice. Little focus is placed on the peculiarities of digital technologies as new specific institutions, as well as on institutions (according to T. Veblen) as patterns of thinking and acting. The already existing concepts not reflect the patterns of human behavior, different from formal institutions. Cyber immunity is defined as a system of interrelated institutions: digital technologies as institutions, i.e. technological knowledge, skills, and abilities as the basis for technological rules (algorithms of actions), formal rules, and patterns of thinking and acting. The latter are able to reduce transaction costs connected with the actors' opportunistic behavior and ensure stable, constructive and effective functioning of the digital economy.

The digital economy as a cybernizing, internetizing mechanism, the global digital economy, as well as national digital economies (Russia and other countries) needs the formation of cyber immunity, the creation of a significant quantum computer. A number of Russian specialists, incl. A.S. Petrenko, ensuring cyber immunity is associated with the creation of a significant quantum computer.

To combat the ever-increasing cyber fraud and other risks and challenges of the digital economy, it is proposed to develop a cyber security system and form a cyber immune system.

References

1. Bank of Russia. (2021). Proekt osnovnyh napravlenij cifrovizacii finansovogo rynka na period 2022-2024 godov [Project of main directions of financial market digitalization for the period 2022-2024]. Moscow, Russian Federation: Bank of Russia, 2022. 38 p. URL: https://www.cbr.ru/Content/Document/File/131360/oncfr_2022-2024.pdf
2. Bank of Russia. (2022a). Kriptovaljuty: trendy, riski, mery [Cryptocurrencies: trends, risks, measures]. Moscow: Bank of Russia. 36 p. URL: https://www.cbr.ru/Content/Document/File/132241/Consultation_Paper_20012022.pdf
3. Bank of Russia. (2022b). Razvitie rynka cifrovyh aktivov v Rossii: doklad dlja obshhestvennyh konsultacij [Development of the digital assets market in Russia: report for public consultations]. Moscow: Bank of Russia. 32 p. URL: https://www.cbr.ru/press/event/?id=14281
4. Bank of Russia. (2023). Infrastruktura finansovogo rynka [Financial market infrastructure]. URL: http://cbr.ru/registries/infrastr/#a_132564
5. Davidson, S., De Filippi, P., & Potts, J. (2018). Blockchains and the economic institutions of capitalism. Journal of Institutional Economics, 14(4), 639-658.
6. De Filippi, P., Hassan, S. (2016). Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code. First Monday, 21(12). URL: https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657
7. FATF (2021). Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris: FATF. URL: www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html
8. Federal Law of July 31, 2020 N 259-FZ "On digital financial assets, digital currency and on amendments to certain legislative acts of the Russian Federation". URL: http://www.consultant.ru/document/cons_doc_LAW_358753/
9. Frolov, D. (2021). Blockchain and institutional complexity: An extended institutional approach. Journal of Institutional Economics, 17(1), 21-36. URL: http://dx.doi.org/10.1017/S1744137420000272

10. Kulikova, K., Koroljov, N. (2023, 20 January). Nadzor kriptchal [Supervision went crypto]. “Commersant” Newspaper, (10), 8. Retrieved from URL: https://www.kommersant.ru/doc/5774896
11. Petrenko, A.S. (2023). Kvantovo-ustojchivyj blokchejn: kak obespechit' bezopasnost' blokchejn-jekosistem i platform v uslovijah atak s ispol'zovaniem kvantovogo komp'jutera [Quantum-resistant blockchain: how to ensure the security of blockchain ecosystems and platforms in the face of attacks using a quantum computer]. St. Petersburg: Piter publishing. 320 p.
12. Robinson, J. (1979). The economics of imperfect competition (Repr. d. 2. 1969 ed.). London: Macmillan. 352 p.
13. Schwab, K. (2018). Tehnologii Chetvertoj promyshlennoj revoljucii [Shaping the Fourth Industrial Revolution]. Moscow: EKSMO. 320 p.
14. Tjotkin, M. (2019, 14 February). Bank JP Morgan vypustit svoju kriptovaljutu [JP Morgan to issue own cryptocurrency]. RBC. URL: https://www.rbc.ru/crypto/news/5c65670b9a794739097b8ca1
15. Vakhitova G. (2023, 04 July). German Negljad: Rossija odna iz nemnogih stran, kotoraja imeet svoju programmu dlja analiza kriptovaljutnyh tranzakcij [German Neglyad: Russia is one of the few countries that has its own software for analyzing cryptocurrency transactions]. Rossiyskaya Gazeta, 144 (9089). URL: https://rg.ru/2023/07/04/dokazatelstva-na-lico.html
16. Yudina, T.N., Lemeshchenko, P.S., & Kupchishina, E.V. (2022). Features of new institutions in the digital economy (digital trust, cyber, information and digital economic security, artificial intelligence). Journal of Institutional Studies, 14(3), 31-45. http://dx.doi.org/10.17835/2076-6297.2022.14.3.031-045

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ БЛОКЧЕЙНА В ФИНАНСОВОМ СЕКТОРЕ РОССИИ В КОНТЕКСТЕ КИБЕРБЕЗОПАСНОСТИ И КИБЕРИММУНИТЕТА

Юдина Тамара Николаевна

Доктор экономических наук, профессор
Московский государственный университет имени М.В. Ломоносова, факультет глобальных процессов, кафедра теории и технологий управления
Москва, Российская Федерация
orchidflower@list.ru

Купчишина Елена Валерьевна

Московский государственный университет имени М.В. Ломоносова, факультет государственного управления, кафедра экономики инновационного развития, соискатель учёной степени кандидата экономических наук
Москва, Российская Федерация
sigrdriva@inbox.ru

Аннотация

Блокчейн в России представляет собой важнейшую ключевую сквозную цифровую технологию, на основе которой запускается цифровой рубль как фудициарные цифровые национальные деньги. Цель исследования: раскрыть роль блокчейна, квантовых технологий и компьютеров в выработке кибериммунитета в России. Результаты исследования: особенностью использования блокчейна в финансовом секторе РФ является создание фиатного цифрового рубля, а не криптовалют как частных квазиденег. Выводы: предложена оригинальная гипотеза обеспечения кибербезопасности блокчейн-экосистем и платформ финансового сектора РФ в условиях нарастающей киберпреступности в контексте выработки им кибериммунитета; в России, как и во всём мире, не выработан кибериммунитет – необходима «квантовая прививка».

Ключевые слова

блокчейн; финансовый сектор Российской Федерации; кибериммунитет

Литература

1. Вахитова Г. Герман Негляд: Россия одна из немногих стран, которая имеет свою программу для анализа криптовалютных транзакций. Российская газета. 04.07.2023 №144 (9089). URL: https://rg.ru/2023/07/04/dokazatelstva-na-lico.html (дата обращения 04.07.2023).
2. Инфраструктура финансового рынка. М.: Банк России, 2023. URL: http://cbr.ru/registries/infrastr/#a_132564 (дата обращения 14.10.2023).
3. Криптовалюты: тренды, риски, меры. М.: Банк России, 2022. 36 с. URL: https://www.cbr.ru/Content/Document/File/132241/Consultation_Paper_20012022.pdf (дата обращения 08.01.2023).
4. Куликова К., Королев Н. Надзор криптчал. Газета «Коммерсантъ». 20.01.2023. №10. с.8. URL: https://www.kommersant.ru/doc/5774896 (дата обращения 20.01.2023).
5. Петренко А.С. Квантово-устойчивый блокчейн: как обеспечить безопасность блокчейн-экосистем и платформ в условиях атак с использованием квантового компьютера. СПб: издательство Питер, 2023. 320 с.
6. Проект основных направлений цифровизации финансового рынка на период 2022-2024 годов. М.: Банк России, 2022. 38 с. URL: https://www.cbr.ru/Content/Document/File/131360/oncfr_2022-2024.pdf (дата обращения 08.01.2023).
7. Развитие рынка цифровых активов в России: доклад для общественных консультаций. Банк России. 07.11.2022. URL: https://www.cbr.ru/press/event/?id=14281 (дата обращения 08.11.2022).

8. Теткин М. Банк JP Morgan выпустит свою криптовалюту. РБК. 14.02.2019. URL: https://www.rbc.ru/crypto/news/5c65670b9a794739097b8ca1 (дата обращения 10.11.2022).
9. Федеральный закон от 31.07.2020 N 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации». URL: http://www.consultant.ru/document/cons_doc_LAW_358753/ (дата обращения 08.11.2022).
10. Шваб К. Технологии четвертой промышленной революции: [перевод с английского] / Клаус Шваб, Николас Дэвис. М.: Эксмо. 2018. 320 с.
11. Юдина Т.Н., Лемещенко П.С., Купчишина Е.В. Особенности новых институтов в цифровой экономике // Journal of Institutional Studies (Журнал институциональных исследований). 2022. № 3. С. 31-45. DOI: 10.17835/2076-6297.2022.14.3.031-045.
12. Davidson S., De Filippi P., Potts J. Blockchains and the economic institutions of capitalism // Journal of Institutional Economics. 2018. Vol. 14. No. 4. P. 639-658.
13. De Filippi P., Hassan S. Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code // First Monday. 2016. Vol. 21. No. 12. URL: https://firstmonday.org/ojs/index.php/fm/article/view/7113/5657 (дата обращения 10.01.2023).
14. FATF. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris: FATF, 2021. URL: www.fatf-gafi.org/publications/fatfrecommendations/documents/Updated-Guidance-RBA-VA-VASP.html (дата обращения 15.11.2022).
15. Frolov D. Blockchain and institutional complexity: An extended institutional approach // Journal of Institutional Economics. 2021. Vol. 17. No. 1. P. 21-36. URL: http://dx.doi.org/10.1017/S1744137420000272 (дата обращения 15.11.2022).
16. Robinson J. The economics of imperfect competition (Repr. d. 2. 1969 ed.). London: Macmillan, 1979. 352 p.